UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

TWENTIETH CENTURY FOX FILM CORP., *et al*. *Plaintiffs*, v. MEGAUPLOAD LIMITED, *et al*., *Defendants*.	No. 1:14cv362 (LO / IDD)

RESPONSE OF DEFENDANT MEGAUPLOAD LTD.
TO PLAINTIFFS' NOTICE OF POTENTIAL LOSS OF EVIDENCE

Defendant Megaupload Limited ("Megaupload") hereby responds to *Plaintiffs' Notice of Potential Loss of Evidence* (Dkt. No. 53) as follows:

Earlier this year, in connection with Defendants' motion to extend the stay, the parties independently had discussions with non-party Cogent Communications, Inc. ("Cogent") regarding the cached data on servers Cogent had leased to Defendants (*see* Dkt. Nos. 48 – 51). Suffice it to say that both sides were under the impression that the data in Cogent's possession was still being preserved and was accessible. Based on the parties' respective representations and arguments, the Court extended the stay, did not allow expedited discovery or enter a preservation order, but directed the parties to advise the Court if any of them learns that "potential evidence in this case, including digital evidence curing being held by [Cogent] is being or might be destroyed." (Dkt. No. 52.) Recently, the parties have each been advised by Cogent that it has been unable to read eight of the sixteen computer hard drives on which the Megaupload cached data have been stored.

Just as Cogent had reported to Plaintiffs, Megaupload's counsel also has been advised that the problem may be mechanical—that is, the "drive heads" may be "frozen"—and that this does not necessarily mean that the data has actually been lost. Without the assistance of a computer forensic expert, however, Cogent cannot confirm that the data remains extant and uncorrupted. Cogent has advised Megaupload's counsel that it is "unwilling" to voluntarily incur the expense to diagnose and fix any mechanical problem or to access and recover the data on the eight drives at issue.

It cannot be gainsaid that the data at issue appears relevant to the private copyright infringement actions—including this one—brought against Megaupload and others. Moreover, the data appears relevant to the defense of the criminal action pending against Megaupload and others, which adds to the urgency of the need to implement reliable forensic techniques to diagnose, repair, and recover the data, as well as to establish a chain of custody, to enable meaningful access by the defense, and to securely store the originals and any mirrored copies.

To address the problem with the Cogent drives, Plaintiffs propose that either they be permitted to serve a subpoena on Cogent to obtain the data or that "the Court appoint an independent computer forensics vendor to verify the integrity of the data and to copy and preserve it for the benefit of the parties while this case otherwise remains stayed." (Dkt. No. 53 at 2.) These are the same proposals previously made by Plaintiffs (Dkt. No. 50) to which Megaupload has already responded (Dkt. No. 51). Megaupload renews its opposition to those proposals and incorporates its prior response by reference. Neither of Plaintiffs' proposals is proper or workable, even if the only concern were the preservation of evidence for use in the civil copyright cases. When the concerns of the criminal case are added in, the proper solution needs to address those complications.

As explained in Megaupload's reply brief (Dkt. No. 51), instead of Plaintiffs' proposals, Megaupload respectfully submits that the Court should direct the parties in the civil cases, Cogent, and the government to meet and confer with United States Magistrate Judge John F. Anderson, who is familiar with this matter, to discuss and devise an appropriate solution to repair the Cogent drives and preserve the evidence on the Cogent servers, as well as to secure and preserve other digital evidence.

ARGUMENT

As Megaupload previously argued at length, simply allowing the transfer of this data to Plaintiffs—whether by subpoena or through a forensic preservation order—is not proper. Instead, Megaupload made a five-point proposal, the details of which would be mediated with the Magistrate Judge's assistance, that balanced the parties' respective interests in the data, as well as protected the privacy interests of customers whose information would be contained in that data (Dkt. No. 51 at 9-10). Megaupload renews that proposal—and, in fact, expands it to now include the government for the reasons explained below.

The need to preserve digitally stored data is not unique to the Cogent servers. A similar issue has arisen in the parallel criminal action. *United States v. Kim Dotcom, et al*., No. 1:12-cr-00003-LO (E.D. Va. filed Jan. 5, 2012) ("*Criminal Action*"). Non-party Carpathia Hosting, Inc. ("Carpathia") owns 1,103 servers, containing 25 petabytes (25 million gigabytes) of data, which had been leased to Megaupload. Non-party QTS Realty Trust, Inc. ("QTS") acquired Carpathia, and hence now controls those servers. In the *Criminal Action*, QTS recently moved for a protective order, seeking to be relieved of the cost and obligation of preserving that data. *Criminal Action*, ECF Nos. 217 & 218. Various interested persons, including Plaintiffs and the government, responded to QTS's motion (*Id*., ECF Nos. 220, 221, 222 & 223), and the Court

required additional submissions (*Id*., ECF No. 229), to which interested persons and the government responded (*Id*., ECF Nos. 230, 232, 233, 234 & 235). The Court still has that matter under advisement. Further discussion of those issues in a meet-and-confer session with the Magistrate Judge should shed further light on the facts and help reveal a fair and just solution.

The unexpected problems with the Cogent drives may be a harbinger of other problems with the preservation of digital evidence. Neither the interests of justice nor the interests of any party or the government would be served if critical digital evidence is lost. In the circumstances of these cases, in which the criminal defendants' assets have been seized and forfeited leaving them unable to access and preserve potentially exculpatory digital evidence, the government may have a constitutional duty under the Due Process Clause to take possession of and preserve the sources of this digital evidence.

As the Court recalls, the government had obtained access to the Carpathia servers and downloaded "selected data" that the government contends was evidence supporting critical allegations made in the superseding indictment. *Criminal Action*, ECF No. 56. By contrast, the criminal defendants (whose assets have been seized and forfeited) presently have no financial means of accessing the Carpathia servers to obtain any exculpatory evidence. If the data on those servers degrades or becomes inaccessible, potentially exculpatory evidence is gone forever. Nonetheless, the government continues to disavow any responsibility either to take possession of the Carpathia servers or to preserve the data thereon. *Criminal Action*, ECF No. 223. As Megaupload showed, however, considerations of due process and fundamental fairness compelled the government to take possession and to ensure preservation of that evidence. *Id.*, ECF No. 221-1. The reasons why bears explication.

It is well-settled that the Due Process Clause "standard of fairness" requires that "criminal defendants be afforded a meaningful opportunity to present a complete defense." *California v. Trombetta*, 467 U.S. 479, 485 (1984). To that end, it is equally well-settled that "the government has a duty to preserve evidence that possesses 'an exculpatory value that was apparent before the evidence was destroyed' where 'the defendant would be unable to obtain comparable evidence by other reasonably available means.'" *United States v. Newsome*, 322 F.3d 328, 334 (4th Cir. 2003) (quoting *Trombetta*, 467 U.S. at 489). In such circumstances, the Government may have a duty "to take affirmative steps to preserve evidence on behalf of criminal defendants," even when the evidence is not already (or is not still) in the government's control. *See Trombetta*, 467 U.S. at 486-87. In the *Criminal Action*, Megaupload contends that the government has a constitutional duty to preserve the Carpathia servers as potentially exculpatory evidence in the defense against the crimes alleged in the superseding indictment.

The test for the government's duty to preserve evidence is whether the "evidence that might be expected to play a significant role in the suspect's defense." *Trombetta*, 467 U.S. at 488. To meet this standard of constitutional "materiality" the evidence "must both possess an exculpatory value that was apparent before the evidence was destroyed, and be of such a nature that the defendant would be unable to obtain comparable evidence by other reasonably available means." *Id*. at 489. In such circumstances, the Government may have a duty "to take affirmative steps to preserve evidence on behalf of criminal defendants," even where the evidence is not already (or still) in the government's control. *See id*. at 486-87. Megaupload contends that after having seized the Carpathia servers to obtain "selected data" that is favorable to the government, the government now has a constitutional duty to preserve the entire data-set

on the Carpathia servers as potentially exculpatory evidence that "might be expected to play a significant role" in the defense against the crimes alleged in the superseding indictment.

The government's duty in this instance becomes clear when the case is contrasted with the facts in *Newsome.* In *Newsome*, the government's failure to seize certain evidence, and the subsequent destruction of that evidence, did not rise to the level of a constitutional violation. There, the defendants were convicted of illegally cutting down certain protected trees in a National Forest. Federal investigators found logs from the protected trees at three local lumber mills. The logs were photographed, and cross-section slabs (or "cookies") of each log were taken and preserved and used as evidence. The full logs were not seized by the federal investigators, however, and the logs were later milled into veneer by the lumber mills. The defendants contended that the government's failure to seize and preserve the full logs constituted spoliation of evidence that violated their Due Process rights.

The Fourth Circuit rejected defendants' contention because the defendants had access to the photographs, the cookies (which were representative samples of the trees and logs), mill records, and mill employees, all of which was deemed to constitute "comparable evidence" that was reasonably available to defendants. *Newsome*, 322 F.3d at 334. Based on that analysis, the Fourth Circuit found no violation of the government's duty to preserve evidence.

The government made a similar argument in the *Criminal Action*, arguing that it took control of the Carpathia servers only temporarily pursuant to a search warrant and obtained certain "selected" samples of the data, which it says it will preserve, but it disclaims any duty to seize and preserve the entirety of the data on those servers. *Criminal Action*, ECF Nos. 56, 82 & 223. That reasoning is fallacious in the circumstances of the *Criminal Action* because the "selected" samples obtained by the government are not representative of all the data on the

Carpathia servers; rather, the "selected data" is only that which (apparently) is consistent with the government's theory of guilt. The government cannot merely allow the remaining data to be lost. There is no other "comparable evidence" available to the criminal defendants if the data on the Carpathia servers is lost.

Having seized control of the Carpathia servers in order to obtain "selected" portions of the data, the government has triggered its duty to preserve the remaining data because the entire data-set "might be significant" to the defense of the *Criminal Action*, and "comparable evidence" cannot be obtained by reasonably available alternative means. Each datum is unique, and unlike the cookies taken in *Newsome*, the government's seizure of a "selected" subset of the data from the Carpathia servers is not a representative sample of the entire data-set.

Similarly, the government has previously taken possession of selected portions of the Cogent data and analyzed it for its own purposes. Specifically, the government reported as follows:[1]

> c. Representatives of the FBI have conducted a preliminary analysis of two of the computer servers located in Washington, D.C., which were owned by Cogent and leased exclusively to the Mega Conspiracy. As of January 19, 2012, approximately 2,444 files were stored on these two servers and were available to the public through the Mega Sites. The preliminary analysis demonstrates that of these 2,444 files, more than 2,200 files had multiple URL links pointing to the same file; more than 550 files had over 100 URL links pointing to the same file; more than 100 files had over 500 URL links pointing to the same file; and approximately 30 files had over 1,000 URL links pointing to the same file.
>
> d. The preliminary analysis further demonstrates that of the 2,444 files, more than 1,000 of the files (roughly 43%) already had at least one copyright infringement takedown request submitted to the Mega Conspiracy indicating that the copy of the copyrighted work was infringing. Because the vast majority of files had multiple URL links pointing to the same file, more than 800 files had been the subject of multiple takedown requests, yet remained accessible through additional URL links. In addition, more than 100 files had over 50 takedown

[1] United States Department of Justice Summary of Evidence In Criminal Case, at 88-89, ¶ 72.c-e, https://www.justice.gov/sites/default/files/usao-edva/legacy/2013/12/20/Mega%20Evidence.pdf.

> requests submitted for each file; and more than 30 files had over 200 takedown requests submitted for each file.
>
> e. In total, the preliminary analysis of the 2,444 files, including content and file name, indicates that at least 90% of the files are infringing copies of non-pornographic copyrighted works; 7% are pornographic videos (many of which are copyrighted); and 3% are unknown due to encryption or because the file has been split into multiple parts.

Thus, as it had done with the Carpathia servers, the government has seized and analyzed a subset of the Cogent cached data, and intends to use that "selected" data as evidence in the *Criminal Action*. Megaupload respectfully submits that having taken possession of the Cogent servers and data to obtain "selected" evidence, the government has triggered its duty under the Due Process Clause to take possession of and preserve all the Cogent data, and make it available to the criminal defendants.

It appears undisputed that all concerned contend that the Cogent data (and Carpathia server data) are relevant to the civil cases. The government has argued that the exculpatory value of that digital evidence is "speculative," but that is mere argument. The interests of justice are best served at this point by implanting reasonable measures to preserve digital evidence so it will be available to all parties for their proposed uses at civil or criminal trials.

Accordingly, Megaupload respectfully submits that the Plaintiffs in this action, as well as the government and the plaintiffs in the other pending copyright infringement actions,[2] should be directed to mediate an appropriate solution to the preservation issues regarding both the Carpathia servers and the Cogent servers. The preservation of this electronically stored evidence is important in all these cases and to all parties, and therefore all parties should be involved.

---

[2] *Microhits, Inc. v. Megaupload, Ltd*., No. 1:12cv327-LO/IDD (E.D. Va. filed Mar. 21, 2012) ("*Microhits Action*"); *Warner Music Group Corp. v. Megaupload, Ltd*., No. 1:14cv374-LO/IDD (E.D. Va. filed Apr. 10, 2014) ("*Warner Music Action*").

Finally, as the Court is aware, the criminal defendants' assets have been seized and, in large part, forfeited under the fugitive disentitlement doctrine. Moreover, the government has previously rejected the suggestion that a portion of the seized assets be released to pay for evidence preservation. Absent a release of seized funds, any costs of forensic repair and preservation would need to be borne by the copyright plaintiffs or the government.

CONCLUSION

Megaupload respectfully submits that the Plaintiffs in this action, as well as the government and the plaintiffs in the other pending copyright infringement actions, should be directed to mediate an appropriate solution to the preservation issues regarding both the Carpathia servers and the Cogent servers.

Dated: May 13, 2016

Respectfully submitted,

/s/ Craig C. Reilly

Craig C. Reilly, Esq. (VSB # 20942)
111 Oronoco Street
Alexandria, Virginia 22314
TEL (703) 549-5354
FAX (703) 549-5355
craig.reilly@ccreillylaw.com

Ira P. Rothken (*pro hac vice*)
Jared R. Smith (*pro hac vice*)
ROTHKEN LAW FIRM
3 Hamilton Landing
Suite 280
Novato, CA 94949
(415) 924-4250
(415) 924-2905 (fax)
ira@techfirm.net

Counsel for Defendant Megaupload, Ltd.

CERTIFICATE OF SERVICE

I hereby certify that on May 13, 2016, the foregoing was filed and served electronically by the Court's CM/ECF system upon all registered users:

Julie M. Carpenter
Kenneth L. Doroshow
Scott B. Wilkens
Erica L. Ross
JENNER & BLOCK LLP
1099 New York Ave., N.W.
Suite 900
Washington, D.C. 20001
Counsel for Plaintiffs

/s/ Craig C. Reilly
Craig C. Reilly, Esq. (VSB # 20942)
111 Oronoco Street
Alexandria, Virginia 22314
TEL (703) 549-5354
FAX (703) 549-5355
craig.reilly@ccreillylaw.com
Counsel for Defendant Megaupload, Ltd.